

COMBATING IDENTITY THEFT A Strategic Plan

limited, and evaluation of effectiveness is almost nonexistent. Although a great deal of useful information is being disseminated, the extent to which the messages are reaching, engaging, or motivating consumers is unclear.

▶ **RECOMMENDATION: INITIATE A MULTI-YEAR PUBLIC AWARENESS CAMPAIGN**

Because consumer education is a critical component of any plan to reduce the incidence of identity theft, the Task Force recommends that member agencies, in the third quarter of 2007, initiate a multi-year national public awareness campaign that builds on the FTC's current "AvoID Theft: Deter, Detect, Defend" campaign, developed pursuant to direction in the FACT Act. This campaign should include the following elements:

- ▶ **Develop a Broad Awareness Campaign.** By broadening the current FTC campaign into a multi-year awareness campaign, and by engaging the Ad Council or similar entities as partners, important and empowering messages should be disseminated more widely and by more partners. The campaign should include public service announcements on the Internet, radio, and television, and in newspapers and magazines, and should address the issue from a variety of perspectives, from prevention through mitigation and remediation, and reach a variety of audiences.
- ▶ **Enlist Outreach Partners.** The agencies conducting the campaign should enlist as outreach partners national organizations either that have been active in helping consumers protect themselves against identity theft, such as the AARP, the Identity Theft Resource Center (ITRC), and the Privacy Rights Clearinghouse (PRC), or that may be well-situated to help in this area, such as the White House Office of Faith-Based and Community Initiatives.
- ▶ **Increase Outreach to Traditionally Underserved Communities.** Outreach to underserved communities should include encouraging language translations of existing materials and involving community-based organizations as partners.
- ▶ **Establish "Protect Your Identity Days."** The campaign should establish "Protect Your Identity Days" to promote better data security by businesses and individual commitment to security by consumers. These "Protect Your Identity Days" should also build on the popularity of community "shred-ins" by encouraging community and business organizations to shred documents containing personal information.



RECOMMENDATION: DEVELOP AN ONLINE CLEARINGHOUSE¹ FOR CURRENT EDUCATIONAL RESOURCES

The Task Force recommends that in the third quarter of 2007, the Task Force member agencies develop an online “clearinghouse” for current identity theft educational resources for consumers, businesses, and law enforcement from a variety of sources at *www.idtheft.gov*. This would make the materials immediately available in one place to any public or private entity willing to launch an education program, and to any citizen interested in accessing the information. Rather than recreate content, entities could link directly to the clearinghouse for timely and accurate information. Educational materials should be added to the website on an ongoing basis.

B. PREVENTION: MAKING IT HARDER TO MISUSE CONSUMER DATA

Keeping valuable consumer data out of the hands of criminals is the first step in reducing the incidence of identity theft. But, because no security is perfect and thieves are resourceful, it is essential to reduce the opportunities for criminals to misuse the data they do manage to steal.

An identity thief who wants to open new accounts in a victim’s name must be able to (1) provide identifying information to enable the creditor or other grantor of benefits to access information on which to base an eligibility decision, and (2) convince the creditor or other grantor of benefits that he is, in fact, the person he purports to be. For example, a credit card grantor processing an application for a credit card will use the SSN to access the consumer’s credit report to check his creditworthiness, and may rely on photo documents, the SSN, and/or other proof to access other sources of information intended to “verify” the applicant’s identity. Thus, the SSN is a critical piece of information for the thief, and its wide availability increases the risk of identity theft.

Identity systems follow a two-fold process: first, determining (“identification”) and setting (“enrollment”) the identity of an individual at the onset of the relationship; and second, later ensuring that the individual is the same person who was initially enrolled (“authentication”). With the exception of banks, savings associations, credit unions, some broker-dealers, mutual funds, futures commission merchants, and introducing brokers (collectively, “financial institutions”), there is no generally-applicable legal obligation on private sector entities to use any particular means of identification. Financial institutions are required to follow certain verification procedures pursuant to regulations promulgated by the federal bank regulatory agencies, the Department of

Treasury, the SEC, and the CFTC under the USA PATRIOT Act.⁶⁷ The regulations require these financial institutions to establish a Customer Identification Program (CIP) specifying identifying information that will be obtained from each customer when accounts are opened (which must include, at a minimum, name, date of birth, address, and an identification number such as an SSN). The CIP requirement is intended to ensure that financial institutions form a reasonable belief that they know the true identity of each customer who opens an account. The government, too, is making efforts to implement new identification mechanisms. For example, REAL ID is a nationwide effort intended to prevent terrorism, reduce fraud, and improve the reliability and accuracy of identification documents that state governments issue.⁶⁸ See Volume II, Part G, for a description of recent laws relating to identification documents.

The verification process can fail, however, in a number of ways. First, identity documents may be falsified. Second, checking the identifying information against other verifying sources of information can produce varying results, depending on the accuracy of the initial information presented and the accuracy or quality of the verifying sources. The process also can fail because employees are trained improperly or fail to follow proper procedures. Identity thieves exploit each of these opportunities to circumvent the verification process.⁶⁹

Once an individual's identity has been verified, it must be authenticated each time he wants the access for which he was initially verified, such as access to a bank account. Generally, businesses authenticate an individual by requiring him to present some sort of credential to prove that he is the same individual whose identity was originally verified. A credential is generally one or more of the following:

- Something a person knows—most commonly a password, but also may be a query that requires specific knowledge only the customer is likely to have, such as the exact amount of the customer's monthly mortgage payment.
- Something a person has—most commonly a physical device, such as a Universal Serial Bus (USB) token, a smart card, or a password-generating device.⁷⁰
- Something a person is—most commonly a physical characteristic, such as a fingerprint, iris, face, and hand geometry. This type of authentication is referred to as biometrics.⁷¹

Some entities use a single form of authentication—most commonly a password—but if it is compromised, there are no other fail-safes in the system. To address this problem, the federal bank regulatory agencies issued guidance promoting stronger customer authentication methods for certain high-risk transactions. Such methods are to include the use of multi-factor authentication, layered security, or other similar controls

reasonably calculated to mitigate the exposure from any transactions that are identified as high-risk. The guidance more broadly provides that banks, savings associations, and credit unions conduct risk-based assessments, evaluate customer awareness programs, and develop security measures to reliably authenticate customers remotely accessing Internet-based financial services.⁷² Financial institutions covered by the guidance were advised that the agencies expected them to have completed the risk assessment and implemented risk mitigation activities by year-end 2006.⁷³ Along with the financial services industry, other industries have begun to implement new authentication procedures using different types of credentials.

SSNs have many advantages and are widely used in our current marketplace to match consumers with their records (including their credit files) and as part of the authentication process. Keeping the authentication process convenient for consumers and credit grantors without making it too easy for criminals to impersonate consumers requires a fine balance. Notwithstanding improvements in certain industries and companies, efforts to facilitate the development of better ways to authenticate consumers without undue burden would help prevent criminals from profiting from their crime.



RECOMMENDATION: HOLD WORKSHOPS ON AUTHENTICATION

Because developing more reliable methods of authenticating the identities of individuals would make it harder for identity thieves to open new accounts or access existing accounts using other individuals' information, the Task Force will hold a workshop or series of workshops, involving academics, industry, and entrepreneurs, focused on developing and promoting improved means of authenticating the identities of individuals. These experts will discuss the existing problem and examine the limitations of current processes of authentication. With that information, the Task Force will probe viable technological and other solutions that will reduce identity fraud, and identify needs for future research. Such workshops have been successful in developing creative and timely responses to consumer protection issues, and the workshops are expected to be useful for both the private and public sectors. For example, the federal government has an interest as a facilitator of the development of new technologies and in implementing technologies that better protect the data it handles in providing benefits and services, and as an employer.

As noted in the Task Force's interim recommendations to the President, the FTC and other Task Force member agencies will host the first such workshop in the second quarter of 2007. The Task Force also recommends that a report be issued or subsequent workshops be held to report on any proposals or best practices identified during the workshop series.

RECOMMENDATION: DEVELOP COMPREHENSIVE RECORD ON PRIVATE SECTOR USE OF SSNs

As noted in Section III A 1, above, the Task Force recommends developing a comprehensive record on the uses of the SSN in the private sector and evaluating their necessity.

C. VICTIM RECOVERY: HELPING CONSUMERS REPAIR THEIR LIVES

Because identity theft can be committed despite the best of precautions, an essential step in the fight against this crime is ensuring that victims have the knowledge, tools, and assistance necessary to minimize the damage and begin the recovery process. Currently, consumers have a number of rights and available resources, but they may not be aware of them.

1. VICTIM ASSISTANCE: OUTREACH AND EDUCATION

Federal and state laws offer victims of identity theft an array of tools to avoid or mitigate the harms they suffer. For example, under the FACT Act, victims can: (1) place alerts on their credit files; (2) request copies of applications and other documents used by the thief; (3) request that the credit reporting agencies block fraudulent trade lines on credit reports; and (4) obtain information on the fraudulent accounts from debt collectors.

In some cases, the recovery process is relatively straightforward. Consumers whose credit card numbers have been used to make unauthorized purchases, for example, typically can get the charges removed without undue burden. In other cases, however, such as those involving new-account fraud, recovery can be an ordeal.

Widely-available guidance advises consumers of steps to take if they have become victims of identity theft, or if their personal information has been breached. For example, the FTC's website, www.ftc.gov/idtheft, contains step-by-step recovery information for victims, as well as for those who may be at risk following a compromise of their data. Many other agencies and organizations link directly to the FTC site and themselves provide education and assistance to victims.

Fair and Accurate Credit Transaction Act (FACT Act) Rights

The Fair and Accurate Credit Transactions Act of 2003 added new sections to the Fair Credit Reporting Act that provide a number of new tools for victims to recover from identity theft. These include the right to place a fraud alert with the credit reporting agencies and receive a free copy of the credit report. An initial alert lasts for 90 days. A victim with an identity theft report documenting actual misuse of the consumer information is entitled to place a 7-year alert on his file. In addition, under the FACT Act, victims can request copies of documents relating to fraudulent transactions, and can obtain information from a debt collector regarding a debt fraudulently incurred in the victim's name. Victims who have a police report also can ask that fraudulent accounts be blocked from their credit report, and can prevent businesses from reporting information that resulted from identity theft to the credit reporting agencies.

Identity theft victims, and consumers who suspect that they may become victims because of lost data, are advised to act quickly to prevent or minimize harm. The steps are straightforward:

- Contact one of the three major credit reporting agencies to place a fraud alert on their credit file. The agencies are required to transmit this information to the other two companies. Consumers who place this 90-day alert are entitled to a free copy of their credit report. Fraud alerts are most useful when a consumer's SSN is compromised, creating the risk of new account fraud.
- Contact any creditors where fraudulent accounts were opened or charges were made to dispute these transactions, and follow up in writing.
- Report actual incidents of identity theft to the local police department and obtain a copy of the police report. This document will be essential to exercising other remedies.
- Report the identity theft incident to the ID Theft Data Clearinghouse by filing a complaint online at ftc.gov/idtheft, or calling toll free 877-ID THEFT. The complaint will be entered into the Clearinghouse and shared with the law enforcement agencies who use the database to investigate and prosecute identity crimes.
- Some states provide additional protections to identity theft victims by allowing them to request a "credit freeze," which prevents consumers' credit reports from being released without their express consent. Because most companies obtain a credit report from a consumer before extending credit, a credit freeze will likely prevent the extension of credit in a consumer's name without the consumer's express permission.

State governments also provide assistance to victims. State consumer protection agencies, privacy agencies, and state Attorneys General provide victim information and guidance on their websites, and some provide personal assistance as well. A number of states have established hotlines, counseling, and other assistance for victims of identity theft. For example, the Illinois Attorney General's office has implemented an Identity Theft Hotline; each caller is assigned a consumer advocate to assist with the recovery process and to help prevent further victimization.

A number of private sector organizations also provide critical victim assistance. Not-for-profit groups such as the Privacy Rights Clearinghouse (PRC) and the Identity Theft Resource Center (ITRC) offer counseling and assistance for identity theft victims who need help in going through the recovery process. The Identity Theft Assistance Center (ITAC), a victim assistance program established by the financial services industry, has helped approximately 13,000 victims resolve problems with disputed accounts and other fraud related to identity theft since its founding in 2004. Finally, many individual companies have established hotlines, distributed materials, and provided special services for customers whose information has been misused. Indeed, some companies rely on their identity theft services as marketing tools.

Despite this substantial effort by the public and private sectors to educate and assist victims, there is room for improvement. Many victims are not aware, or do not take advantage, of the resources available to them. For example, while the FTC receives roughly 250,000 contacts from victims every year, that number is only a small percentage of all identity theft victims. Moreover, although first responders could be a key resource for identity theft victims, the first responders often are overworked and may not have the information that they need about the steps for victim recovery. It is essential, therefore, that public and private outreach efforts be expanded, better coordinated, and better funded.

RECOMMENDATION: PROVIDE SPECIALIZED TRAINING ABOUT VICTIM RECOVERY TO FIRST RESPONDERS AND OTHERS PROVIDING DIRECT ASSISTANCE TO IDENTITY THEFT VICTIMS

First responders and others who provide direct assistance and support to identity theft victims must be adequately trained. Accordingly, the Task Force recommends the following:

- ▶ **Train Local Law Enforcement Officers.** By the third quarter of 2007, federal law enforcement agencies, which could include the U.S. Postal Inspection Service, the FBI, the Secret Service, and the FTC, should conduct training seminars—delivered in person, online, or via video—for local law enforcement officers on available resources and providing assistance for victims.
- ▶ **Provide Educational Materials for First Responders That Can Be Readily Used as a Reference Guide for Identity Theft Victims.** During the third quarter of 2007, the FTC and DOJ should develop a reference guide, which should include contact information for resources and information on first steps to recovery, and should make that guide available to law enforcement officers through the online clearinghouse at

www.idtheft.gov. Such guidance would assist first responders in directing victims on their way to recovery.

- ▶ **Distribute an Identity Theft Victim Statement of Rights.** Federal law provides substantial assistance to victims of identity theft. From obtaining a police report to blocking fraudulent accounts in a credit report, consumers—as well as law enforcement, private businesses, and other parties involved in the recovery process—need to know what remedies are available. Accordingly, the Task Force recommends that, during the third quarter of 2007, the FTC draft an ID Theft Victim Statement of Rights, a short and simple statement of the basic rights victims possess under current law. This document should then be disseminated to victims through law enforcement, the financial sector, and advocacy groups, and posted at *www.idtheft.gov*.
- ▶ **Develop Nationwide Training for Victim Assistance Counselors.** Crime victims receive assistance through a wide array of federal and state-sponsored programs, as well as nonprofit organizations. Additionally, every United States Attorney's Office in the country has a victim-witness coordinator who is responsible for referring crime victims to the appropriate resources to resolve harms that resulted from the misuse of their information. All of these counselors should be trained to respond to the specific needs of identity theft victims, including assisting them in coping with the financial and emotional impact of identity crime. Therefore, the Task Force recommends that a standardized training curriculum for victim assistance be developed and promoted through a nationwide training campaign, including through DOJ's Office for Victims of Crime (OVC). Already, OVC has begun organizing training workshops, the first of which was held in December 2006. These workshops are intended to train not only victim-witness coordinators from U.S. Attorney's Offices, but also state, tribal, and local victim service providers. The program will help advocates learn how to assist victims in self-advocacy and how and when to intervene in a victim's recovery process. Training topics will include helping victims deal with the economic and emotional ramifications of identity theft, assisting victims with understanding how an identity theft case proceeds through the criminal justice system, and identity theft laws. Additional workshops should be held in 2007.



**RECOMMENDATION: DEVELOP AVENUES FOR
INDIVIDUALIZED ASSISTANCE TO IDENTITY THEFT VICTIMS**

Although many victims are able to resolve their identity theft-related issues without assistance, some individuals would

benefit from individualized counseling. The availability of personalized assistance should be increased through national service organizations, such as those using retired seniors or similar groups, and pro bono activities by lawyers, such as those organized by the American Bar Association (ABA). In offering individualized assistance to identity theft victims, these organizations and programs should use the victim resource guides that are already available through the FTC and DOJ's Office for Victims of Crime. Specifically, the Task Force also recommends the following:

- ▶ **Engage the American Bar Association to Develop a Program Focusing on Assisting Identity Theft Victims with Recovery.** The ABA has expertise in coordinating legal representation in specific areas of practice through law firm volunteers. Moreover, law firms have the resources and expertise to staff an effort to assist victims of identity theft. Accordingly, the Task Force recommends that, beginning in 2007, the ABA, with assistance from the Department of Justice, develop a pro bono referral program focusing on assisting identity theft victims with recovery.

2. MAKING IDENTITY THEFT VICTIMS WHOLE

Identity theft inflicts many kinds of harm upon its victims, making it difficult for them to feel that they ever will recover fully. Beyond tangible forms of harm, statistics cannot adequately convey the emotional toll that identity theft often exacts on its victims, who frequently report feelings of violation, anger, anxiety, betrayal of trust, and even self-blame or hopelessness. These feelings may continue, or even increase, as victims work through the credit recovery and criminal justice processes. Embarrassment, cultural factors, or personal or family circumstances (e.g., if the victim has a relationship to the identity thief) may keep the victims from reporting the problem to law enforcement, in turn making them ineligible to take advantage of certain remedies. Often, these reactions are intensified by the ongoing, long-term nature of the crime. Criminals may not stop committing identity theft after having been caught; they simply use information against the same individual in a new way, or they sell the information so that multiple identity thieves can use it. Even when the fraudulent activity ceases, the effects of negative information on the victim's credit report can continue for years.

The many hours victims spend in attempting to recover from the harms they suffer often takes a toll on victims that is not reflected in their monetary losses. One reason that identity theft can be so destructive to its victims is the sheer amount of time and energy often required to recover from the offense, including having to correct credit reports, dispute charges with individual creditors, close and reopen bank accounts, and monitor credit reports for future problems arising from the theft.

"I received delinquent bills for purchases she [the suspect] made. I spent countless hours on calls with creditors in Texas who were reluctant to believe that the accounts that had been opened were fraudulent. I spent days talking to police in Texas in an effort to convince them that I was allowed by Texas law to file a report and have her [the suspect] charged with the theft of my identity... I had to send more than 50 letters to the creditors to have them remove the more than 60 inquiries that were made by this woman..."

Nicole Robinson
Testimony before
House Ways and
Means Committee,
Subcommittee on
Social Security
May 22, 2001

In addition to losing time and money, some identity theft victims suffer the indignity of being mistaken for the criminal who stole their identities, and have been wrongfully arrested.⁷⁴ In one case, a victim's driver's license was stolen, and the information from the license was used to open a fraudulent bank account and to write more than \$10,000 in bad checks. The victim herself was arrested when local authorities thought she was the criminal. In addition to the resulting feelings of trauma, this type of harm is a particularly difficult one for an identity theft victim to resolve.



RECOMMENDATION: AMEND CRIMINAL RESTITUTION STATUTES TO ENSURE THAT VICTIMS RECOVER FOR THE VALUE OF TIME SPENT IN ATTEMPTING TO REMEDIATE THE HARMS THEY SUFFERED

Restitution to victims from convicted thieves is available for the direct financial costs of identity theft offenses. However, there is no specific provision in the federal restitution statutes for compensation for the time spent by victims recovering from the crime, and court decisions interpreting the statutes suggest that such recovery would be precluded.

As stated in the Task Force's interim recommendations to the President, the Task Force recommends that Congress amend the federal criminal restitution statutes to allow for restitution from a criminal defendant to an identity theft victim, in an amount equal to the value of the victim's time reasonably spent attempting to remediate the intended or actual harm incurred from the identity theft offense. The language of the proposed amendment is in Appendix C. DOJ transmitted the proposed amendment to Congress on October 4, 2006.



RECOMMENDATION: EXPLORE THE DEVELOPMENT OF A NATIONAL PROGRAM ALLOWING IDENTITY THEFT VICTIMS TO OBTAIN AN IDENTIFICATION DOCUMENT FOR AUTHENTICATION PURPOSES

One of the problems faced by identity theft victims is proving that they are who they say they are. Indeed, some identity theft victims have been mistaken for the criminal who stole their identity, and have been arrested based on warrants issued for the thief who stole their personal data. To give identity theft victims a means to authenticate their identities in such a situation, several states have developed identification documents, or "passports," that authenticate identity theft victims. These voluntary mechanisms are designed to prevent the misuse of the victim's name in the

criminal justice system when, for example, an identity thief uses his victim's name when arrested. These documents often use multiple factors for authentication, such as biometric data and a password. The FBI has established a similar system through the National Crime Information Center, allowing identity theft victims to place their name in an "Identity File." This program, too, is limited in scope. Beginning in 2007, the Task Force member agencies should lead an effort to study the feasibility of developing a nationwide system allowing identity theft victims to obtain a document that they can use to avoid being mistaken for the suspect who has misused their identity. The system should build on the programs already used by several states and the FBI.

3. GATHERING BETTER INFORMATION ON THE EFFECTIVENESS OF VICTIM RECOVERY MEASURES

Identity theft victims have been granted many new rights in recent years. Gathering reliable information about the utility of these new rights is critical to evaluating whether they are working well or need to be modified. Additionally, because some states have measures in place to assist identity theft victims that have no federal counterpart, it is important to assess the success of those measures to determine whether they should be adopted more widely. Building a record of victims' experiences in exercising their rights is therefore crucial to ensuring that any strategy to fight identity theft is well-supported.

RECOMMENDATION: ASSESS EFFICACY OF TOOLS AVAILABLE TO VICTIMS

The Task Force recommends the following surveys or assessments:

- ▶ **Conduct Assessment of FACT Act Remedies Under FCRA.** The FCRA is among the federal laws that enable victims to restore their good name. The FACT Act amendments to the FCRA provide several new rights and tools for actual or potential identity theft victims, including the availability of credit file fraud alerts; the blocking of fraudulent trade lines on credit reports; the right to have creditors cease furnishing information relating to fraudulent accounts to credit reporting agencies; and the right to obtain business records relating to fraudulent accounts. Many of these rights have been in effect for a short time. Accordingly, the Task Force recommends that the agencies with enforcement authority for these statutory provisions assess their impact and effectiveness through appropriate surveys. Agencies should report on the results in calendar year 2008.

- ▶ **Conduct Assessment of State Credit Freeze Laws.** Among the state-enacted remedies without a federal counterpart is one granting consumers the right to obtain a credit freeze. Credit freezes make a consumer's credit report inaccessible when, for example, an identity thief attempts to open an account in the victim's name. State laws differ in several respects, including whether all consumers can obtain a freeze or only identity theft victims; whether credit reporting agencies can charge the consumer for unfreezing a file (which would be necessary when applying for credit); and the time allowed to the credit reporting agencies to unfreeze a file. These provisions are relatively new, and there is no "track record" to show how effective they are, what costs they may impose on consumers and businesses, and what features are most beneficial to consumers. An assessment of how these measures have been implemented and how effective they have been would help policy makers in considering whether a federal credit freeze law would be appropriate. Accordingly, the Task Force recommends that the FTC, with support from the Task Force member agencies, assess the impact and effectiveness of credit freeze laws, and report on the results in the first quarter of 2008.

D. LAW ENFORCEMENT: PROSECUTING AND PUNISHING IDENTITY THIEVES

The two keys to preventing identity theft are (1) preventing access to sensitive consumer information through better data security and increased education, and (2) preventing the misuse of information that may be obtained by would-be identity thieves. Should those mechanisms fail, strong criminal law enforcement is necessary to both punish and deter identity thieves.

The increased awareness about identity theft in recent years has made it necessary for many law enforcement agencies at all levels of government to devote additional resources to investigating identity theft-related crimes. The principal federal law enforcement agencies that investigate identity theft are the FBI, the United States Secret Service, the United States Postal Inspection Service, SSA OIG, and ICE. Other agencies, as well as other federal Inspectors General, also may become involved in identity theft investigations.

In investigating identity theft, law enforcement agencies use a wide range of techniques, from physical surveillance to financial analysis to computer forensics. Identity theft investigations are labor-intensive, and because no single investigator can possess all of the skill sets needed to handle each of these functions, the investigations often require multiple detectives, analysts, and agents. In addition, when a suspected identity

In September 2006, the Michigan Attorney General won the conviction of a prison inmate who had orchestrated an elaborate scheme to claim tax refunds owed to low income renters through the state's homestead property tax program. Using thousands of identities, the defendant and his cohorts were detected by alert U.S. Postal carriers who were suspicious of the large number of Treasury checks mailed to certain addresses.

theft involves large numbers of potential victims, investigative agencies may need additional personnel to handle victim-witness coordination and information issues.

During the last several years, federal and state agencies have aggressively enforced the laws that prohibit the theft of identities. All 50 states and the District of Columbia have some form of legislation that prohibits identity theft, and in all those jurisdictions, except Maine, identity theft can be a felony. See Volume II, Part H, for a description of state criminal law enforcement efforts. In the federal system, a wide range of statutory provisions is used to investigate and prosecute identity theft including, most notably, the aggravated identity theft statute⁷⁵ enacted in 2004, which carries a mandatory two-year prison sentence. Since then, DOJ has made increasing use of the aggravated identity theft statute: in Fiscal Year 2006, DOJ charged 507 defendants with aggravated identity theft, up from 226 defendants charged with aggravated identity theft in Fiscal Year 2005. In many of these cases, the courts have imposed substantial sentences. See Volume II, Part I, for a description of sentencing in federal identity theft prosecutions.

The Department of Justice also has initiated many special identity theft initiatives in recent years. The first of these, in May 2002, involved 73 criminal prosecutions by U.S. Attorney's Offices against 135 individuals in 24 federal districts. Since then, identity theft has played an integral part in several initiatives that DOJ and other agencies have directed at online economic crime. For example, "Operation Cyber Sweep," a November 2003 initiative targeting Internet-related economic crime, resulted in the arrest or conviction of more than 125 individuals and the return of indictments against more than 70 people involved in various types of Internet-related fraud and economic crime. See Volume II, Part J, for a description of special enforcement and prosecution initiatives.

1. COORDINATION AND INTELLIGENCE/INFORMATION SHARING

Federal law enforcement agencies have recognized the importance of coordination among agencies and of information sharing between law enforcement and the private sector. Coordination has been challenging, however, for several reasons: identity theft data currently reside in numerous databases; there is no standard reporting form for all identity theft complaints; and many law enforcement agencies have limited resources. Given these challenges, law enforcement has responded to the need for greater cooperation by, among other things, forming interagency task forces and developing formal intelligence-sharing mechanisms. Law enforcement also has worked to develop methods of facilitating the timely receipt and analysis of identity theft complaint data and other intelligence.

In a "Operation Firewall," the Secret Service was responsible for the first-ever takedown of a large illegal online bazaar. Using the website www.shadowcrew.com, the Shadowcrew organization had thousands of members engaged in the online trafficking of stolen identity information and documents, such as drivers' licenses, passports, and Social Security cards, as well as stolen credit card, debit card, and bank account numbers. The Shadowcrew members trafficked in at least 1.7 million stolen credit card numbers and caused total losses in excess of \$4 million. The Secret Service successfully shut down the website following a year-long undercover investigation, which resulted in the arrests of 21 individuals in the United States on criminal charges in October 2004. Additionally, law enforcement officers in six foreign countries arrested or searched eight individuals.

a. Sources of Identity Theft Information

Currently, federal law enforcement has a number of sources of information about identity theft. The primary source of direct consumer complaint data is the FTC, which, through its Identity Theft Clearinghouse, makes available to law enforcement through a secure website the complaints it receives. Internet-related identity theft complaints also are received by the Internet Crime Complaint Center (IC3), a joint venture of the FBI and National White Collar Crime Center. The IC3 develops case leads from the complaints it receives and sends them to law enforcement throughout the country. Additionally, a special component of the FBI that works closely with the IC3 is the Cyber Initiative and Resource Fusion Unit (CIRFU). The CIRFU, based in Pittsburgh, facilitates the operation of the National Cyber Forensic Training Alliance (NCFTA), a public/private alliance and fusion center, by maximizing intelligence development and analytical resources from law enforcement and critical industry partners. The U.S. Postal Inspection Service also hosts its Financial Crimes Database, a web-based national database available to U.S. Postal Service inspectors for use in analyzing mail theft and identity theft complaints received from various sources. These are but a few of the sources of identity theft data for law enforcement. See Volume II, Part K, for a description of how law enforcement obtains and analyzes identity theft data.

Private sector entities—including the financial services industry and credit reporting agencies—also are important sources of identity theft information for law enforcement agencies. They often are best positioned to identify early anomalies in various components of the e-commerce environment in which their businesses interact, which may represent the earliest indicators of an identity theft scenario. For this reason and others, federal law enforcement has undertaken numerous public- and private-sector collaborations in recent years to improve information sharing. For example, corporations have placed analysts and investigators with IC3 in support of initiatives and investigations. In addition, ITAC, the cooperative initiative of the financial services industry, shares information with law enforcement and the FTC to help catch and convict the criminals responsible for identity theft. See Volume II, Part K, for a description of other private sector sources of identity theft data. Such alliances enable critical industry experts and law enforcement agencies to work together to more expeditiously receive and process information and intelligence vital both to early identification of identity theft schemes and rapid development of aggressive investigations and mitigation strategies, such as public service advisories. At the same time, however, law enforcement agencies report that they have encountered obstacles in obtaining support and assistance from key private-sector stakeholders in some cases, absent legal process, such as subpoenas, to obtain information.

One barrier to more complete coordination is that identity theft information resides in multiple databases, even within individual law enforcement agencies. A single instance of identity theft may result in information being posted at federal, state, and local law enforcement agencies, credit reporting agencies, credit issuers, financial institutions, telecommunications companies, and regulatory agencies. This, in turn, leads to the inefficient “stove-piping” of relevant data and intelligence. Additionally, in many cases, agencies do not or cannot share information with other agencies, making it difficult to determine whether an identity theft complaint is related to a single incident or a series of incidents. This problem may be even more pronounced at the state and local levels.

b. Format for Sharing Information and Intelligence

A related issue is the inability of the primary law enforcement agencies to communicate electronically using a standard format, which greatly impedes the sharing of criminal law enforcement information. When data collection systems use different formats to describe the same event or fact, at least one of the systems must be reprogrammed to fit the other program’s terms. Where several hundred variables are involved, the programming resources required to connect the two databases can be an insurmountable barrier to data exchange.

To address that concern, several law enforcement organizations, including the International Association of Chiefs of Police’s (IACP) Private Sector Liaison Committee and the Major Cities’ Chiefs (MCC), have recommended developing a standard electronic identity theft police report form. Reports that use a standard format could be shared among law enforcement agencies and stored in a national repository for investigatory purposes.

c. Mechanisms for Sharing Information

Law enforcement uses a variety of mechanisms to facilitate information sharing and intelligence analysis in identity-theft investigations. See Volume II, Part L, for a description of federal law enforcement outreach efforts. As just one example, the Regional Information Sharing Systems (RISS) Program is a long-standing, federally-funded program to support regional law enforcement efforts to combat identity theft and other crimes. Within that program, law enforcement has established intelligence-sharing systems. These include, for example, the Regional Identity Theft Network (RITNET), created to provide Internet-accessible identity theft information for federal, state, and local law enforcement agencies within the Eastern District of Pennsylvania. RITNET is designed to include data from the FTC, law enforcement agencies, and the banking industry, and allow investigators to connect crimes committed in various jurisdictions

and link investigators. It also will collect information on all reported frauds, regardless of size, thereby eliminating the advantage identity thieves have in keeping theft amounts low.

Multi-agency working groups and task forces are another successful investigative approach, allowing different agencies to marshal resources, share intelligence, and coordinate activities. Federal authorities lead or co-lead over 90 task forces and working groups devoted (in whole or in part) to identity theft. See Volume II, Part M, for a description of interagency working groups and task forces.


Despite these efforts, coordination among agencies can be improved. Better coordination would help law enforcement officers “connect the dots” in investigations and pool limited resources.



RECOMMENDATION: ESTABLISH A NATIONAL IDENTITY THEFT LAW ENFORCEMENT CENTER

The Task Force recommends that the federal government establish, as resources permit, an interagency National Identity Theft Law Enforcement Center to better consolidate, analyze, and share identity theft information among law enforcement agencies, regulatory agencies, and the private sector. This effort should be led by the Department of Justice and include representatives of federal law enforcement agencies, including the FBI, the Secret Service, the U.S. Postal Inspection Service, the SSA OIG, and the FTC. Leveraging existing resources, increased emphasis should be placed on the analysis of identity theft complaint data and other information and intelligence related to identity theft from public and private sources, including from identity theft investigations. This information should be made available to appropriate law enforcement at all levels to aid in the investigation, prosecution, and prevention of identity theft crimes, including to target organized groups of identity thieves and the most serious offenders operating both in the United States and abroad. Effective mechanisms that enable law enforcement officers from around the country to share, access, and search appropriate law enforcement information around-the-clock, including through remote access, should also be developed. As an example, intelligence from documents seized during investigations could help facilitate the ability of agents and officers to “connect the dots” between various investigations around the country.

In a case prosecuted by the United States Attorney's Office for the Eastern District of Pennsylvania, a gang purchased 180 properties using false or stolen names. The thieves colluded to procure inflated appraisals for the properties, obtained financing, and drained the excess profits for their own benefit, resulting in harm to the identity theft victims and to the neighborhood when most of the properties went into foreclosure.

**RECOMMENDATION: DEVELOP AND PROMOTE THE ACCEPTANCE OF A UNIVERSAL IDENTITY THEFT REPORT FORM**

The Task Force recommended in its interim recommendations that the federal government, led by the FTC, develop and promote a universal police report like that recommended by the IACP and MCC—a standard document that an identity theft victim could complete, print, and take to any local law enforcement agency for verification and incorporation into the police department's report system. This would make it easier for victims to obtain these reports, facilitate entry of the information into a central database that could be used by law enforcement to analyze patterns and trends, and initiate more investigations of identity theft.

Criminal law enforcers, the FTC, and representatives of financial institutions, the consumer data industry, and consumer advocacy groups have worked together to develop a standard form that meets this need and captures essential information. The resulting Identity Theft Complaint ("Complaint") form was made available in October 2006 via the FTC's Identity Theft website, www.ftc.gov/idtheft. Consumers can print copies of their completed Complaint and take it to their police station, where it can be used as the basis for a police report. The Complaint provides much greater specificity about the details of the crime than would a typical police report, so consumers will be able to submit it to credit reporting agencies and creditors to assist in resolving their identity theft-related problems. Further, the information they enter into the Complaint will be collected in the FTC's Identity Theft Data Clearinghouse, thus enriching this source of consumer complaints for law enforcement. This system also relieves the burden on local law enforcement because consumers are completing the detailed Complaint before filing their police report.

**RECOMMENDATION: ENHANCE INFORMATION SHARING BETWEEN LAW ENFORCEMENT AND THE PRIVATE SECTOR**

Because the private sector in general, and financial institutions in particular, are an important source of identity theft-related information for law enforcement, the Task Force recommends the following steps to enhance information sharing between law enforcement and the private sector:

- ▶ **Enhance Ability of Law Enforcement to Receive Information From Financial Institutions.** Section 609(e) of the Fair Credit Reporting Act enables identity theft victims to receive identity theft-related documents and to designate law enforcement agencies to receive the documents on their behalf. Despite that fact, law enforcement agencies have sometimes encountered difficulties in obtaining such information without a subpoena. By the second quarter of 2007, DOJ should initiate discussions with the financial sector to ensure greater compliance with this law, and should include other law enforcement agencies in these discussions. DOJ, on an ongoing basis, should compile any recommendations that may result from those discussions and, where appropriate, relay those recommendations to the appropriate private or public sector entity for action.
- ▶ **Initiate Discussions With the Financial Services Industry on Countermeasures to Identity Thieves.** Federal law enforcement agencies, led by the U.S. Postal Inspection Service, should continue discussions with the financial services industry as early as the second quarter of 2007 to develop more effective fraud prevention measures to deter identity thieves who acquire data through mail theft. Discussions should include use of the Postal Inspection Service's current Financial Industry Mail Security Initiative. The Postal Inspection Service, on an ongoing basis, should compile any recommendations that may result from those discussions and, where appropriate, relay those recommendations to the appropriate private or public sector entity for action.
- ▶ **Initiate Discussions With Credit Reporting Agencies On Preventing Identity Theft.** By the second quarter of 2007, DOJ should initiate discussions with the credit reporting agencies on possible measures that would make it more difficult for identity thieves to obtain credit based on access to a victim's credit report. The discussions should include other law enforcement agencies, including the FTC. DOJ, on an ongoing basis, should compile any recommendations that may result from the discussions and, where appropriate, relay the recommendations to the appropriate private or public sector entity for action.

2. COORDINATION WITH FOREIGN LAW ENFORCEMENT

Federal enforcement agencies have found that a significant portion of the identity theft committed in the United States originates in other countries. Therefore, coordination and cooperation with foreign law enforcement is essential. A positive step by the United States in ensuring

such coordination was the ratification of the Convention on Cybercrime (2001). The Cybercrime Convention is the first multilateral instrument drafted to address the problems posed by the spread of criminal activity on computer networks, including offenses that relate to the stealing of personal information and the exploitation of that information to commit fraud. The Cybercrime Convention requires parties to establish laws against these offenses, to ensure that domestic laws give law enforcement officials the necessary legal authority to gather electronic evidence, and to provide international cooperation to other parties in the fight against computer-related crime. The United States participated in the drafting of the Convention and, in November 2001, was an early signatory.

Because of the international nature of many forms of identity theft, providing assistance to, and receiving assistance from, foreign law enforcement on identity theft is critical for U.S. enforcement agencies. Under current law, the United States generally is able to provide such assistance, which fulfills our obligations under various treaties and enhances our ability to obtain reciprocal assistance from foreign agencies. Indeed, there are numerous examples of collaborations between U.S. and foreign law enforcement in identity theft investigations.

Nevertheless, law enforcement faces several impediments in their ability to coordinate efforts with foreign counterparts. First, even though federal law enforcement agencies have successfully identified numerous foreign suspects trafficking in stolen consumer information, their ability to arrest and prosecute these criminals is very limited. Many countries do not have laws directly addressing identity theft, or have general fraud laws that do not parallel those in the United States. Thus, investigators in the United States may be able to prove violations of American identity theft statutes, yet be unable to show violations of the foreign country's law. This can impact cooperation on extradition or collection of evidence necessary to prosecute offenders in the United States. Additionally, some foreign governments are unwilling to cooperate fully with American law enforcement representatives, or may cooperate but fail to aggressively prosecute offenders or seize criminal assets.

Second, certain statutes governing foreign requests for electronic and other evidence—specifically, 18 U.S.C. § 2703 and 28 U.S.C. § 1782—fail to make clear whether, how, and in which court certain requests can be fulfilled. This jurisdictional uncertainty has impeded the ability of American law enforcement officers to assist their counterparts in other countries who are conducting identity theft investigations.

The FBI Legal Attache in Bucharest recently contributed to the development and launch of www.efrauda.ro, a Romanian government website for the collection of fraud complaints based on the IC3 model. The IC3 also provided this Legal Attache with complaints received by U.S. victims who were targets of a Romanian Internet crime ring. The complaint forms provided to Romanian authorities via the Legal Attache assisted the Romanian police and Ministry of Justice with the prosecution of Romanian subjects.



RECOMMENDATION: ENCOURAGE OTHER COUNTRIES TO ENACT SUITABLE DOMESTIC LEGISLATION CRIMINALIZING IDENTITY THEFT

The Department of Justice, after consulting with the Department of State, should formally encourage other countries to enact suitable domestic legislation criminalizing identity theft. A number of countries already have adopted, or are considering adopting, criminal identity-theft offenses. In addition, since 2005, the United Nations Crime Commission (UNCC) has convened an international Expert Group to examine the worldwide problem of fraud and identity theft. That Expert Group is drafting a report to the UNCC (for presentation in 2007) that is expected to describe the major trends in fraud and identity theft in numerous countries and to offer recommendations on best practices by governments and the private sector to combat fraud and identity theft. DOJ should provide input to the Expert Group concerning the need for the criminalization of identity theft worldwide.



RECOMMENDATION: FACILITATE INVESTIGATION AND PROSECUTION OF INTERNATIONAL IDENTITY THEFT BY ENCOURAGING OTHER NATIONS TO ACCEDE TO THE CONVENTION ON CYBERCRIME, OR TO ENSURE THAT THEIR LAWS AND PROCEDURES ARE AT LEAST AS COMPREHENSIVE

Global acceptance of the Convention on Cybercrime will help to assure that all countries have the legal authority to collect electronic evidence and the ability to cooperate in trans-border identity theft investigations that involve electronic data. The U.S. government should continue its efforts to promote universal accession to the Convention and assist other countries in bringing their laws into compliance with the Convention's standards. The Department of State, in close coordination with the Department of Justice and Department of Homeland Security, should lead this effort through appropriate bilateral and multilateral outreach mechanisms. Other agencies, including the Department of Commerce and the FTC, should participate in these outreach efforts as appropriate. This outreach effort began years ago in a number of international settings, and should continue until broad international acceptance of the Convention on Cybercrime is achieved.

► **RECOMMENDATION: IDENTIFY COUNTRIES THAT HAVE BECOME SAFE HAVENS FOR PERPETRATORS OF IDENTITY THEFT AND TARGET THEM FOR DIPLOMATIC AND ENFORCEMENT INITIATIVES FORMULATED TO CHANGE THEIR PRACTICES.**

Safe havens for perpetrators of identity theft and individuals who aid and abet such illegal activities should not exist. However, the inaction of law enforcement agencies in some countries has turned those countries into breeding grounds for sophisticated criminal networks devoted to identity theft. Countries that tolerate the existence of such criminal networks encourage their growth and embolden perpetrators to expand their operations. In 2007, the U.S. law enforcement community, with input from the international law enforcement community, should identify the countries that are safe havens for identity thieves. Once identified, the U.S. government should use appropriate diplomatic measures and any suitable enforcement mechanisms to encourage those countries to change their practices.

► **RECOMMENDATION: ENHANCE THE U.S. GOVERNMENT'S ABILITY TO RESPOND TO APPROPRIATE FOREIGN REQUESTS FOR EVIDENCE IN CRIMINAL CASES INVOLVING IDENTITY THEFT**

The Task Force recommends that Congress clarify which courts can respond to appropriate foreign requests for electronic and other evidence in criminal investigations, so that the United States can better provide prompt assistance to foreign law enforcement in identity theft cases. This clarification can be accomplished by amending 18 U.S.C. § 2703 and making accompanying amendments to 18 U.S.C. §§ 2711 and 3127, and by enacting a new statute, 18 U.S.C. § 3512, which would supplement the foreign assistance authority of 28 U.S.C. § 1782. Proposed language for these legislative changes is available in Appendix D (text of amendments to 18 U.S.C. §§ 2703, 2711, and 3127, and text of new language for 18 U.S.C. § 3512).



**RECOMMENDATION: ASSIST, TRAIN, AND SUPPORT FOREIGN
LAW ENFORCEMENT**

Because the investigation of major identity theft rings increasingly will require foreign cooperation, federal law enforcement agencies, led by DOJ, FBI, Secret Service, USPIS, and ICE, should assist, train, and support foreign law enforcement through the use of Internet intelligence-collection entities, including IC3 and CIRFU, and continue to make it a priority to work with other countries in joint investigations targeting identity theft. This work should begin in the third quarter of 2007.

3. PROSECUTION APPROACHES AND INITIATIVES

As part of its effort to prosecute identity theft aggressively, DOJ, since 2002, has conducted a number of enforcement initiatives that have focused, in whole or in part, on identity theft. In addition to broader enforcement initiatives led by DOJ, various individual U.S. Attorney's Offices have undertaken their own identity theft efforts. For example, the U.S. Attorney's Office in the District of Oregon has an identity theft "fast track" program that requires eligible defendants to plead guilty to aggravated identity theft and agree, without litigation, to a 24-month minimum mandatory sentence. Under this program, it is contemplated that defendants will plead guilty and be sentenced on the same day, without the need for a pre-sentence report to be completed prior to the guilty plea, and waive all appellate and post-conviction remedies. In exchange for their pleas of guilty, defendants are not charged with the predicate offense, such as bank fraud or mail theft, which would otherwise result in a consecutive sentence under the United States Sentencing Guidelines. In addition, two U.S. Attorney's Offices have collaborated on a special initiative to combat passport fraud, known as Operation Checkmate. See Volume II, Part J.

Notwithstanding these efforts, challenges remain for federal law enforcement. Because of limited resources and a shortage of prosecutors, many U.S. Attorney's Offices have monetary thresholds—i.e., requirements that a certain amount of monetary loss must have been suffered by the victims—before the U.S. Attorney's Office will open an identity theft case. When a U.S. Attorney's Office declines to open a case based on a monetary threshold, investigative agents cannot obtain additional information through grand jury subpoenas that could help to uncover more substantial monetary losses to the victims.

RECOMMENDATION: INCREASE PROSECUTIONS OF IDENTITY THEFT

The Task Force recommends that, to further increase the number of prosecutions of identity thieves, the following steps should be taken:

- ▶ **Designate An Identity Theft Coordinator for Each United States Attorney's Office To Design a Specific Identity Theft Program for Each District.** DOJ should direct that each U.S. Attorney's Office, by June 2007, designate one Assistant U.S. Attorney who should serve as a point of contact and source of expertise within that office for other prosecutors and agents. That Assistant U.S. Attorney also should assist each U.S. Attorney in making a district-specific determination about the areas on which to focus to best address the problem of identity theft. For example, in some southwest border districts, identity theft may be best addressed by stepping up efforts to prosecute immigration fraud. In other districts, identity theft may be best addressed by increasing prosecutions of bank fraud schemes or by making an effort to add identity theft violations to the charges that are brought against those who commit wire/mail/bank fraud schemes through the misappropriation of identities.
- ▶ **Evaluate Monetary Thresholds for Prosecution.** By June 2007, the investigative agencies and U.S. Attorney's Offices should re-evaluate current monetary thresholds for initiating identity theft cases and, specifically, should consider whether monetary thresholds for accepting such cases for prosecution should be lowered in light of the fact that investigations often reveal additional loss and additional victims, that monetary loss may not always adequately reflect the harm suffered, and that the aggravated identity theft statute makes it possible for the government to obtain significant sentences even in cases where precisely calculating the monetary loss is difficult or impossible.
- ▶ **Encourage State Prosecution of Identity Theft.** DOJ should explore ways to increase resources and training for local investigators and prosecutors handling identity theft cases. Moreover, each U.S. Attorney, by June 2007, should engage in discussions with state and local prosecutors in his or her district to encourage those prosecutors to accept cases that do not meet appropriately-set thresholds for federal prosecution, with the understanding that these cases need not always be brought as identity theft cases.

- ▶ **Create Working Groups and Task Forces.** By the end of 2007, U.S. Attorneys and investigative agencies should create or make increased use of interagency working groups and task forces devoted to identity theft. Where funds for a task force are unavailable, consideration should be given to forming working groups with non-dedicated personnel.

▶ **RECOMMENDATION: CONDUCT TARGETED ENFORCEMENT INITIATIVES**

Law enforcement agencies should continue to conduct enforcement initiatives that focus exclusively or primarily on identity theft. The initiatives should pursue the following:

- ▶ **Unfair or Deceptive Means to Make SSNs Available for Sale.** Beginning immediately, law enforcement should more aggressively target the community of businesses on the Internet that sell individuals' SSNs or other sensitive information to anyone who provides them with the individual's name and other limited information. The SSA OIG and other agencies also should continue or initiate investigations of entities that use unlawful means to make SSNs and other sensitive personal information available for sale.
- ▶ **Identity Theft Related to the Health Care System.** HHS should continue to investigate identity theft related to Medicare fraud. As part of this effort, HHS should begin to work with state authorities immediately to provide for stronger state licensure and certification of providers, practitioners, and suppliers. Schemes to defraud Medicare may involve the theft of beneficiaries' and providers' identities and identification numbers, the opening of bank accounts in individuals' names, and the submission of fraudulent Medicare claims. Medicare payment is linked to state licensure and certification of providers, practitioners, and suppliers as business entities. Lack of state licensure and certification laws and/or laws that do not require identification and location information of owners and officers of providers, practitioners and suppliers, can hamper the ability of HHS to stop identity theft related to fraudulent billing of the Medicare program.
- ▶ **Identity Theft By Illegal Aliens.** Law enforcement agencies, particularly the Department of Homeland Security, should conduct targeted enforcement initiatives directed at illegal aliens who use stolen identities to enter or stay in the United States.

▶ **RECOMMENDATION: REVIEW CIVIL MONETARY PENALTY PROGRAMS**

By the fourth quarter of 2007, federal agencies, including the SEC, the federal bank regulatory agencies, and the Department of Treasury, should review their civil monetary penalty programs to assess whether they adequately address identity theft. If they do not, analysis should be done as to what, if any, remedies, including legislation, would be appropriate, and any such legislation should be proposed by the first quarter of 2008. If a federal agency does not have a civil monetary penalty program, the establishment of such a program with respect to identity theft should be considered.

4. STATUTES CRIMINALIZING IDENTITY-THEFT RELATED OFFENSES: THE GAPS

Federal law enforcement has successfully investigated and prosecuted identity theft under a variety of criminal statutes. Effective prosecution can be hindered in some cases, however, as a result of certain gaps in those statutes. At the same time, a gap in one aspect of the U.S. Sentencing Guidelines has precluded some courts from enhancing the sentences for some identity thieves whose conduct affected multiple victims. See Volume II, Part N, for an additional description of federal criminal statutes used to prosecute identity theft.

a. The Identity Theft Statutes

The two federal statutes that directly criminalize identity theft are the identity theft statute (18 U.S.C. § 1028(a)(7)) and the aggravated identity theft statute (18 U.S.C. § 1028A(a)). The identity theft statute generally prohibits the possession or use of a means of identification of a person in connection with any unlawful activity that either constitutes a violation of federal law or that constitutes a felony under state or local law.⁷⁶ Similarly, the aggravated identity theft statute generally prohibits the possession or use of a means of identification of another person during the commission of, or in relation to, any of several enumerated federal felonies, and provides for enhanced penalties in those situations.

There are two gaps in these statutes, however. First, because both statutes are limited to the illegal use of a means of identification of "a person," it is unclear whether the government can prosecute an identity thief who misuses the means of identification of a corporation or organization, such as the name, logo, trademark, or employer identification number of a legitimate business. This gap means that federal prosecutors cannot use those statutes to charge identity thieves who, for example, create and use

counterfeit documents or checks in the name of a corporation, or who engage in phishing schemes that use an organization's name. Second, the enumerated felonies in the aggravated identity theft statute do not include certain crimes that recur in identity theft and fraud cases, such as mail theft, uttering counterfeit securities, tax fraud, and conspiracy to commit certain offenses.

b. Computer-Related Identity Theft Statutes

Two of the federal statutes that apply to computer-related identity theft have similar limitations that preclude their use in certain important circumstances. First, 18 U.S.C. § 1030(a)(2) criminalizes the theft of information from a computer. However, federal courts only have jurisdiction if the thief uses an interstate communication to access the computer (unless the computer belongs to the federal government or a financial institution). As a result, the theft of personal information either by a corporate insider using the company's internal local networks, or by a thief intruding into a wireless network, generally would not involve an interstate communication and could not be prosecuted under this statute. In one case in North Carolina, for instance, an individual broke into a hospital computer's wireless network and thereby obtained patient information. State investigators and the victim asked the United States Attorney's Office to support the investigation and charge the criminal. Because the communications occurred wholly intrastate, however, no federal law criminalized the conduct.

A second limitation is found in 18 U.S.C. § 1030(a)(5), which criminalizes actions that cause "damage" to computers, i.e., that impair the "integrity or availability" of data or computer systems.⁷⁷ Absent special circumstances, the loss caused by the criminal conduct must exceed \$5,000 to constitute a federal crime. Many identity thieves obtain personal information by installing malicious spyware, such as keyloggers, on many individuals' computers. Whether the programs succeed in obtaining the unsuspecting computer owner's financial data, these sorts of programs harm the "integrity" of the computer and data. Nevertheless, it is often difficult or impossible to measure the loss this damage causes to each computer owner, or to prove that the total value of these many small losses exceeds \$5,000.

c. Cyber-Extortion Statute

Another federal criminal statute that may apply in some computer-related identity theft cases is the "cyber-extortion" provision of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(7). This provision, which prohibits the transmission of a threat "to cause damage to a protected computer,"⁷⁸ is used to prosecute criminals who threaten to delete data,